ESnet
ENERGY SCIENCES NETWORK

Zone-Hopping!

A Practical Solution to DNSSEC Zone-Walking

Fatema Bannat Wala
Security Engineer @ESnet
Lawrence Berkeley National Laboratory

Dr. Stephan Bohacek
Electrical & Computer Engineering
University of Delaware

U.S. DEPARTMENT OF ENERGY
Office of Science

BERKELEY LAB

Motivation

What/Why DNSSEC?

- DNSSEC was introduced to provide integrity of DNS records. Using PKI, it provides signed DNS records that proves that the records are not tampered in the transit. Prevents MiTM attacks on DNS messages.

Concept of Proof of Denial of existence

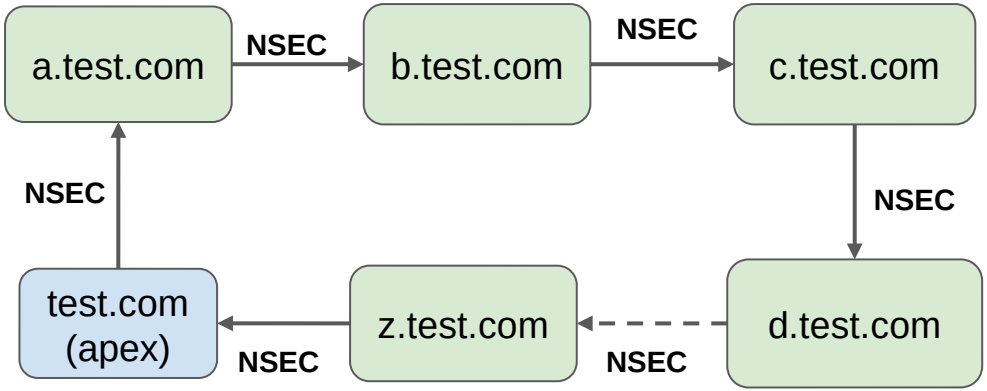
- DNSSEC introduced a new record - NSEC, which is sent as response to non-existence domain queries listing the before and the after domain present at the Auth. server.
- NSEC results in Zone enumeration, commonly known as the Zone-Walking problem (ZW)

Example NSEC -

```
a.test.com          3600    IN    A          192.168.1.1
a.test.com          3600    IN    NSEC    b.test.com A RRSIG NSEC
b.test.com          3600    IN    A          192.168.1.2
b.test.com          3600    IN    NSEC    c.test.com A RRSIG NSEC
```

What is Zone-Walking?

- A process of enumerating the DNS Zone contents by intentionally querying for NXDOMAINs and utilizing the information presented by NSEC records.
- It allows all fully qualified domain names to be identified within a domain.



Currently Available ZW Solutions

- **NSEC3** - Defined in RFC 5155. Instead of returning the plain-text owner name and next available domain name in NSEC record, NSEC3 hashed the values of the owner name and the next existing domain name.
  - Limitations - NSEC3 hashes can be cracked with a success rate of 88%
  - NSEC3 hash validation is computationally expensive.

For Ex, NSEC3 record:

```
s1kfv8ko3dafgetgrfevv5f6h7gjfnfb92lp.test.xyz. 3600      IN NSEC3 1 0
0 - 6FTHPGDTSH1VL6GFTWKM92GS4JRF1RL NS SOA RRSIG DNSKEY
```

- **RFC 4470** - Introduced the concept of "Minimally Covering NSEC Records and DNSSEC On-line Signing".
  - "A new NSEC record is dynamically produced and signed. It has an owner name lexically before the QNAME (queried name) but lexically following any existing name and a "next name" lexically following the QNAME but before any existing name."
  - The new NSEC record hence generated would still cover the non-existent query, but with the fake previous-name and the next name, effectively preventing the disclosure of zone contents.

Two Implementations

NSEC3 White Lies (WL)

- Fake NSEC3 records are generated on-the-fly that surround the requested name.
- The new NSEC3 record will comprise of the hash of the QNAME minus one as owner name and the hash of the QNAME plus one as the next name

Black Lies (BL)

- Different secure negative response "NODATA" instead of "NXDOMAIN".
- An NSEC record is dynamically created where the owner name is the same as the QNAME, and the next name as the immediate lexico. successor of the QNAME

Limitations of WL/BL:

- The private key needs to be available on the internet-accessible zone's authoritative servers
- Generating signatures of NSEC records, on-the-fly, is computationally expensive and makes authoritative servers vulnerable to a denial of service (DoS) attacks.

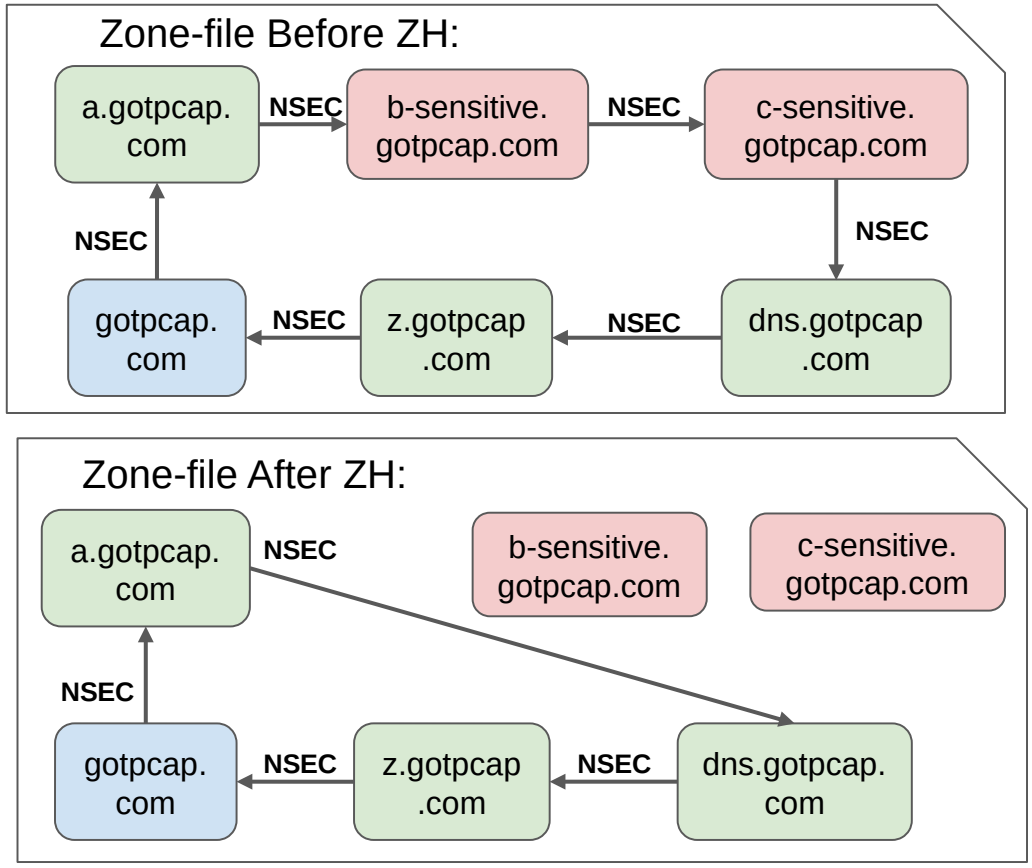
According to Route 53:

- *“If Route 53 Resolver team detects a traffic pattern that matches the ones generated when DNS zones are walked on your endpoint, the service team will throttle the traffic on your endpoint. As a consequence you might observe a high percentage of your DNS queries timing out.”*

Proposed Solution - Zone-Hopping (ZH)

- The objective of our solution is to disable zone walking for specific FQDNs, while still allowing zone walking to find FQDNs that we seek to protect from denial of existence attacks.
- It is a hybrid approach where the “positive” responses are authenticated DNSSEC, while “negative” responses are treated just like in the standard DNS.
- The proposed solution modifies the NSEC records for instantiated names, which are pre-generated and signed in advance (off-line), but in a slightly different manner:
    - public and sensitive records are separated in two files and each is signed separately with the same key, thus creating two zone-files.
    - Then, the NSEC records from the sensitive zone file are deleted, and this modified file is merged back into the public zone file.
    - This process yields a final zone file devoid of NSEC records with sensitive data, effectively preventing their disclosure through zone walking while still serving any requests for the sensitive domains with complete authenticity.

Testing ZH




```
; gotpcap.signed.db. final
; File written on Tue Mar 12 18:06:31 2024
; dnssec_signzone version 9.18.18
gotpcap.com.
                604800  IN SOA gotpcap.com.
                604800  RRSIG  SOA 13 2 604800
                604800  NS     dns.gotpcap.com.
                604800  RRSIG  NS 13 2 604800
                604800  NSEC   a.gotpcap.com.
                604800  RRSIG  NSEC 13 2 604800
                604800  DNSKEY 257 3 13 xS9zESD
                604800  RRSIG  DNSKEY 13 2 604800
a.gotpcap.com.
                604800  IN A    192.168.2.3
                604800  RRSIG  A 13 3 604800
                604800  NSEC   dns.gotpcap.com.
                604800  RRSIG  NSEC 13 3 604800
dns.gotpcap.com.
                604800  IN A    34.125.87.209
                604800  RRSIG  A 13 3 604800
                604800  NSEC   z.gotpcap.com.
                604800  RRSIG  NSEC 13 3 604800
b– sensitive .gotpcap.com.
                604800  IN A    10.10.0.1
                604800  RRSIG  A 13 3 604800
c– sensitive .gotpcap.com.
                604800  IN A    10.10.0.2
                604800  RRSIG  A 13 3 604800
z.gotpcap.com.
                604800  IN A    192.168.2.4
                604800  RRSIG  A 13 3 604800
                604800  NSEC   gotpcap.com.
                604800  RRSIG  NSEC 13 3 604800
```

Result of applying ZH:

We used ldns to zone walk "gotpcap.com". Before applying the solution:

```
#ldns-walk gotpcap.com
gotpcap.com.    gotpcap.com. NS SOA RRSIG NSEC DNSKEY
a.gotpcap.com.      A RRSIG NSEC
b-sensitive.gotpcap.com. A RRSIG NSEC
c-sensitive.gotpcap.com. A RRSIG NSEC
dns.gotpcap.com.    A RRSIG NSEC
z.gotpcap.com.      A RRSIG NSEC
```

Sensitive FQDNs are not longer discovered via zone-walking after ZH:

```
#ldns-walk gotpcap.com
gotpcap.com.    gotpcap.com. NS SOA RRSIG NSEC DNSKEY
a.gotpcap.com.      A RRSIG NSEC
dns.gotpcap.com.    A RRSIG NSEC
z.gotpcap.com.      A RRSIG NSEC
```

But, querying the sensitive FQDNs generates a valid response from the name-server.

```
# dig @34.125.255.60 c-sensitive.gotpcap.com a +multi +dnssec
;;
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43569
;; flags : qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags : do; udp: 1232
;; QUESTION SECTION:
;c- sensitive .gotpcap.com. IN A
;; ANSWER SECTION:
c-sensitive.gotpcap.com. 604709 IN A 10.10.0.2
c-sensitive.gotpcap.com. 604709 IN RRSIG A 13 3 604800
(20240411170631 20240312170631 11305 gotpcap.com.
knx4IK1axo/yZhmw5GfP7m39acCwGdz60NGLPlKxjoFy
h89ixC0TZ/pwEzWTF4bG+s+xPCcXdW2F2FDmuuyDBg== )
```

Comparison of ZW solutions at a glance

Attacks	Standard DNS	DNSSEC+ZH	DNSSEC+NSEC	DNSSEC+NSEC3	DNSSEC+BL/WL
Integrity of records(MiTM)	Susceptible	Immune	Immune	Immune	Immune
DoE	Susceptible	Susceptible	Immune	Immune	Immune
DoS	Susceptible	Susceptible	Susceptible	Susceptible+	Susceptible++
Domain leak	Immune	Immune	Susceptible++	Susceptible+	Immune
Private Key Exposure	N/A	Immune	Immune	Immune	Susceptible

ZH considerations

With advancing technology and internet evolving to support more IPv6 transitions-

- Preventing Zone enumeration will be more critical than before!
- A goto tool to dump valid IPv6 addresses from the Zone-file

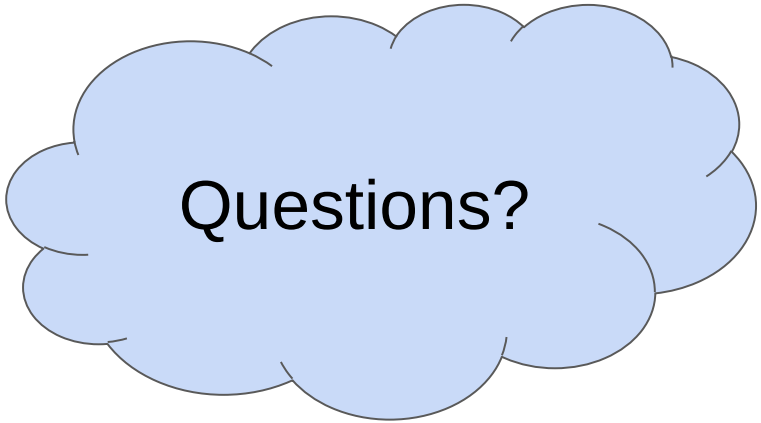
Split-view DNS architecture vs. ZW vs. ZTA-

- An external attacker can quickly discover all publicly facing servers via ZW and, upon gaining access to the private network, the attacker can efficiently discover internal servers, which facilitates lateral movement within the network!

Aggressive Use of DNSSEC-Validated Cache-

- ZH wouldn’t work if the resolver is using aggressive negative cache, for negative responses the standard DNS caching approach should be used so that the entire range between the QNAME and Next name in a single NSEC can’t be DoS’ed. And the negative responses are only returned by the resolver when the matching QNAME that resulted the caching is queried again. Or NSEC with 0 TTL should be used.

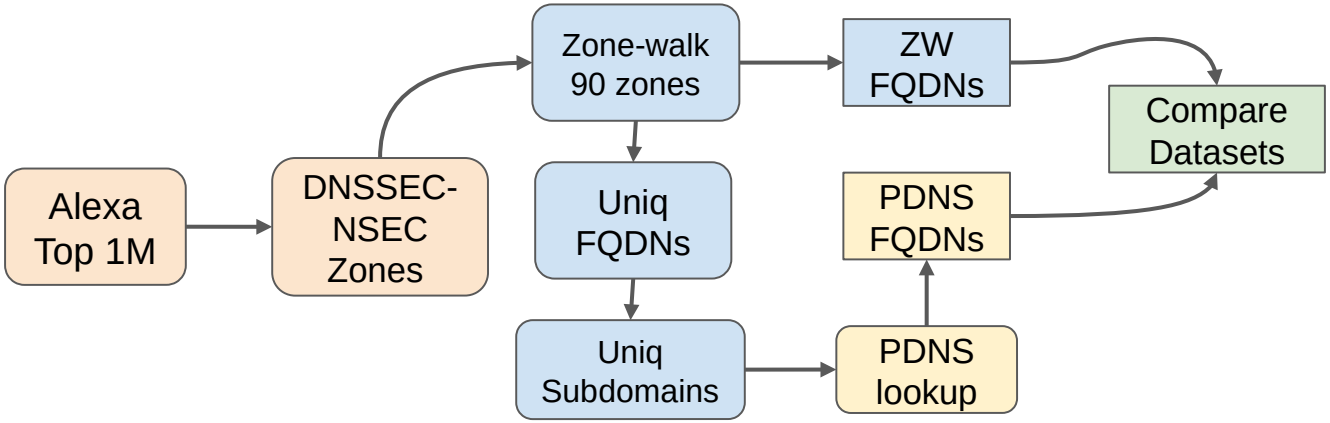
THANK YOU!



Appendix: Assessing the Problem: ZW vs. PDNS

Experimental Setup:

- We did zone-enumeration on 90 dnssec-enabled zones from the list of Alexa Top-1M.
- Extracted the unique FQDNs (561,332) and subdomains (458,227) from the ZW datasets.
- Queried pDNS database for the unique subdomains (177,377) and collected FQDNs available in pDNS database.
- Compared the FQDNs from ZW to the FQDNs collected from the pDNS database.



Comparison Results:

- These results show that data exposed through zone walking is not available from passive listening systems (PDNS).
- Less than 50% of coverage overall in PDNS.
- PDNS systems are “passive”, you need to *know what to query.* Hence, not as straightforward as ZW to enumerate the zone.
- PDNS systems have defenses in place to prevent enumeration, like queries/day, no wildcard searches for the zone ex: *.example.com.

Category	Zones	Subdomains	ZW FQDNs	PDNS FQDNs	pdns Coverage
Gov.	34	30,552	51,845	29,129	56.18%
Academia	14	101,680	147,115	77,265	52.52%
Other	40	45,145	152,654	35,958	23.55%
Total	88	177,377	351,614	142,352	40.48%

Appendix: DoS vs. DoE Argument

- DoE leads to DoS
- DoS is low hanging, low-effort attack to achieve same results as DoE
- Attack complexity - To pull a successful DoE is harder than DoS, but the impact is same.
- Which raises an interesting question -
  - do we even want the DoE protection in DNSSEC, since the protocol is already vulnerable to DoS?
    - Yes? - But at what cost? Zone information leakage!
    - No? - ZH offers best of both worlds: sensitive information is handled just like traditional DNS (i.e. no NSEC records), but at the same time, digital signatures (RRSIG) are available to prove the authenticity of the records.